National Infrastructure Protection Center
CyberNotes

Issue #2002-23 *November 18, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 31 and November 14, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Abuse[1]	Unix	Abuse 2.0	Two buffer overflow vulnerability exists: a vulnerability exists in the "-net" command line option, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability exists when an excessively long commandline argument is submitted, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Abuse Local Buffer Overflows CVE Name: CAN-2002-1250	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ACME Labs Software[2]	Unix	Tiny HTTPD 0.1.0	A Directory Traversal vulnerability exists due to a failure to properly sanitize web requests, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	TinyHTTPD Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Apache Software Foundation[3] ***Debian releases new advisories*** [4, 5, 6]	**Unix**	**Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.6, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.19, 1.3.20, 1.3.22-1.3.27**	**Multiple vulnerabilities exist: several buffer overflow vulnerabilities exist in the 'htdigest' utility due to improper bounds checking when user-supplied data is copied into local buffers, which could possibly let a malicious user execute arbitrary code; a vulnerability exists in the 'htdigest' utility due to insecure system() calls when commandline options are processed, which could let a malicious user execute arbitrary code; and a vulnerability exists because 'htpasswd' temporary files are created insecurely, which could let a malicious user read or corrupt the Apache password file and possibly obtain unauthorized access.**	**No workaround or patch available at time of publishing.** ***Debian:*** **http://security.debian.org/pool/updates/main/a/apache/**	**Multiple Apache Vulnerabilities** **CVE Name: CAN-2002-1233**	**Medium/ High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[1] iDEFENSE Security Advisory, 11.01.02, October 31, 2002.
[2] INetCop Security Advisory, 2002-0x82-001, November 11, 2002.
[3] Bugtraq, October 16, 2002.
[4] Debian Security Advisory, DSA 187-1, November 4, 2002.
[5] Debian Security Advisory, DSA 188-1, November 5, 2002.
[6] Debian Security Advisory, DSA 195-1, November 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apache Software Foundation[7]	Unix	Apache 1.3.26	A vulnerability exists in the 'mod_php' module only if the 'safe_mode' php option is disabled, which could let a remote malicious user obtain file description information.	Unofficial Patch (George Guninski): http://downloads.securityfocus.com/vulnerabilities/patches/guninski-httpd.patch	Apache mod_php File Descriptor Leakage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Arts Core Studios[8]	Windows, Unix	CuteCast 1.2	A vulnerability exists in the default configuration because user information is stored in plaintext in a publicly accessible directory, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CuteCast Plaintext User Information	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
AstroCam [9]	Unix	AstroCam 1.7.1, 1.8, 1.8.5, 1.8.6, 2.0, 2.1, 2.1.2	A vulnerability exists in 'astrocam.cgi' due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://freshmeat.net/redir/astrocam/28903/url_tgz/astrocam.tar.gz&user=cdp_xe	AstroCam Shell Metacharacters Sanitization	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Buffalo Technology [10]	Multiple	AirStation Pro Intelligent Access Point WLM-L11G	A Denial of Service vulnerability exists when certain types of data are submitted to port 80.	No workaround or patch available at time of publishing.	AirStation Pro Intelligent Access Point Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cascade Soft[11]	Multiple	W3Mail 1.0.6 & greater	A vulnerability exists in 'viewAttachment.cgi' because the filename argument is passed to the open() function with being sanitized, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	W3Mail File Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[12]	Multiple	PIX Firewall 6.2.2	A Denial of Service vulnerability exists when TCP SYN packets are sent repeatedly to the subnet address. This occurs only when Telnet/SSH access has been enabled on the firewall for hosts on the internal network.	Upgrade available at: http://www.cisco.com/tac	PIX Firewall Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. There is no exploit code required. A number of available tools may be used to trigger this condition.

[7] Georgi Guninski Security Advisory #58, November 6, 2002.
[8] Bugtraq, November 8, 2002.
[9] SecurityTracker Alert ID 1005523, November 3, 2002.
[10] Arhont Ltd. Information Security Advisory, November 13, 2002
[11] SecurityFocus, November 13, 2002.
[12] Bugtraq, November 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq Computer Corporation[13]	Unix	Tru64 4.0 g PK3 (BL17), 4.0f PK7 (BL18), 5.0a PK3 (BL17), 5.1a PK3 (BL3), 5.1 PK5 (BL19)	A Denial of Service vulnerability exists due to the way IGMP packets are handled.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	Tru64 IGMP Denial of Service	Low	Bug discussed in newsgroups and websites.
CVSup[14]	Multiple	CVSup-mirror 1.2	A symbolic link vulnerability exists in 'cvsupd.out,' which could let a malicious user cause a Denial of Service and potentially obtain elevated privileges.	No workaround or patch available at time of publishing.	CVSup-Mirror Insecure Temporary Files	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Darren Reed[15] ***NetBSD issues advisory*[16]**	**Unix**	**IPFilter 3.1.1-3.1.10, 3.2.1-3.2.22, 3.3.1-3.3.22, 3.4.1-3.4.28**	**A vulnerability exists because under certain circumstances ports can be opened on FTP servers, which could let a malicious user obtain unauthorized access.**	**Upgrade available at: http://coombs.anu.edu.au/~avalon/ip-fil3.4.29.tar.gz** ***NetBSD:*** ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-024.txt.asc	**IPFilter FTP Proxy Unauthorized Access**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
D-Link[17] ***Patch now available*[18]**	**Multiple**	**DWL-900AP+ 2.1, 2.2**	**A vulnerability exists in the TFTP server which could let a remote malicious user obtain sensitive information and potentially full administrative access.**	***Upgrade available at:*** **ftp://ftp.dlink.com/Wireless/DWL900AP+/Firmware/dwl900AP+_firmware_230.exe**	**DWL-900AP+ TFTP Server**	**Medium/ High** **(High if administrative access can be obtained)**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Ehud Gavron[19]	Unix	TrACES route 6.0, 6.1.1	A buffer overflow vulnerability exists in Traceroute-nanog because root privileges that are used to open a raw socket are not relinquished, which could let a malicious user obtain root privileges.	**SuSE:** ftp://ftp.suse.com/pub/suse/	Traceroute-nanog Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[13] Hewlett Packard Security Advisory, SSRT2266, November 13, 2002.
[14] SecurityFocus, November 9, 2002.
[15] SecurityFocus, October 19, 2002.
[16] NetBSD Security Advisory, 2002-024, November 4, 2002.
[17] ETHEREANET-NCC Security Report EN-NCC-20021014-04, October 21, 2002.
[18] SecurityFocus, November 7, 2002.
[19] SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
eZ Systems[20]	Multiple	HTTP Bench 1.1	A vulnerability exists in the php script because the contents of web server readable files are disclosed, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	HTTPBench Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Francisco Burzi[21]	Unix	PHP-Nuke 5.6	A vulnerability exists due to insufficient sanitization of variables used to construct SQL queries, which could let a malicious user corrupt database information and obtain unauthorized access.	Upgrade available at: http://www.phpnuke.org./modules.php?name=Downloads&d_op=getit&lid=321	PHP-Nuke 5.6 SQL Injection CVE Name: CAN-2002-1242	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Frank McIngvale[22, 23]	Unix	LuxMan 0.41	A vulnerability exists in the 'maped' process because 'gzip' is executed without specifying the full path to the executable, which could let a remote malicious user remote obtain read/write access to /dev/mem that could lead to root access on the system.	**Debian:** http://security.debian.org/pool/updates/main/l/luxman/	LuxMan File Path CVE Name: CAN-2002-1245	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Global Sun Technology, Inc.[24]	Multiple	D-Link DWL-900AP+ 2.2; GlobalSunTech WISECOM GL2422AP-0T; Linksys WAP11 2.2	A vulnerability exists in GlobalSunTech access points when a broadcast packet that contains the string,, “gstsearch” is sent to UDP port 27155, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	GlobalSunTech Access Point Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Hewlett Packard Company[25]	Unix	Compaq Tru64 4.0g, Tru64 4.0f, HP TruCluster 1.6	A vulnerability exists in the OSIS V5.4 LDAP Module for System Authentication, which could let a local/remote malicious user obtain unauthorized access.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/v4.0g/osisv54_ssrt2385_40g_patch.tar http://ftp.support.compaq.com/patches/public/unix/v4.0f/osisv54_ssrt2385_40f_patch.tar	Tru64/ TruCluster OSIS V5.4 LDAP Module Unauthorized Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[20] Bugtraq, November 10, 2002.
[21] iDEFENSE Security Advisory, 10.31.02c, October 31, 2002.
[22] iDEFENSE Security Advisory 11.06.02, November 6, 2002.
[23] Debian Security Advisory, DSA 189-1, November 6, 2002.
[24] KHAMSIN Security News, November 3, 2002.
[25] Hewlett Packard Security Advisory, SSRT2385, November 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[26]	Unix	TruCluster Server 5.0A, 5.1A, 5.1	A remote Denial of Service vulnerability exists in the Cluster Interconnect software package.	Hotfix available at: http://ftp.support.compaq.com/patches/public/unix/	TruCluster Server Cluster Interconnect Remote Denial of Service CVE Name: CAN-2002-0711	Low	Bug discussed in newsgroups and websites.
Heysoft[27]	Windows NT	EventSave 5.1, 5.2, EventSave + 5.1, + 5.2	A vulnerability exists because event logs are not properly backed up if the Microsoft Windows Event Viewer is used to view the event log for the current month, which could lead to an inadequate backup log of events.	Upgrade available at: http://www.heysoft.de/nt/eventlog/EventSave.zip	EventSave Event Log Notification	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Hotfoon[28]	Multiple	Hotfoon 4.0	Several vulnerabilities exist: a vulnerability exists because the password is stored in plaintext, which could let a malicious user obtain unauthorized access; and a buffer overflow vulnerability exists in the text input field used for dialing telephone numbers due to inadequate boundary checks, which could let a malicious user cause a Denial of Service and execute arbitrary code.	No workaround or patch available at time of publishing.	Hotfoon Dialer Plain Text Password Storage & Buffer Overflow	Low/ Medium/ **High** **(Medium if unauthorized access can be obtained and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the password vulnerability and a Proof of Concept exploit has been published for the buffer overflow vulnerability.
Hughes Technologies[29]	Unix	LibHTTPD 1.2	A buffer overflow vulnerability exists when an POST request is submitted that is of excessive length, which could let a malicious user execute arbitrary code with super user privileges.	No workaround or patch available at time of publishing.	LibHTTPD POST Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[26] Hewlett Packard Security Bulletin, SSRT2265, November 4, 2002.
[27] Heysoft Security Bulletin, November 1, 2002.
[28] Bugtraq, November 10, 2002.
[29] INetCop Security Advisory, 2002-0x82-003, November 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[30] ***Update available***[31]	**Multiple**	**Infoprint Controller Software 1.0 47012**	**A buffer overflow vulnerability exists in the Telnet based remote management services due to insufficient checks on user-supplied input for the login parameter, which could let a malicious user cause a Denial of Service.** ***Note: This vulnerability has been rectified in later versions of the printer controller software. As it stands, printers installed with the controller software above a certain version are NOT vulnerable (Infoprint 21 - Controller Code Level: 1.056007 - Any newer Infoprint models)***	**No workaround or patch available at time of publishing.**	**Infoprint Printers Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Incognito Software Inc.[32]	Multiple	iSMTP Gateway 5.0.1	A buffer overflow vulnerability exists due to insufficient bounds checking on user-supplied input, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	Contact Incognito Software Inc for information about obtaining the latest version of the software.	ISMTP Gateway Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Iomega[33]	Unix	NAS A300U	Multiple vulnerabilities exist: a vulnerability exists because administrative authentication credentials are sent across the network in plaintext, which could let an unauthorized remote malicious user obtain access to the administrative interface; a vulnerability exists because LANMAN authentication credentials are sent across the network in plaintext and may be intercepted by attackers with the ability to sniff network traffic; and a vulnerability exists because FTP access to the shared directories can be disabled, however, this does not disable FTP access to the NAS but only to the shared directories, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	NAS A300U Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[30] Securiteam, October 25, 2002.
[31] Bugtraq, October 31, 2002.
[32] Bugtraq, November 11, 2002.
[33] Bugtraq, November 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ISC[34, 35, 36, 37, 38, 39, 40]	Unix	FreeBSD FreeBSD 4.4-4.7; ISC BIND 8.1-8.1.2, 8.2-8.2.6, 8.3.0-8.3.3; OpenBSD OpenBSD 3.0-3.2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in 'named' when responses are constructed using previously-cached malformed SIG records, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists due to a failure to properly handle DNS lookups for non-existent sub-domains when overly large OPT resource records are appended to a query; and remote Denial of Service vulnerability exists due to a failure to properly dereference cache SIG RR elements that contain invalid expiry times from the internal database.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:43/bind.patch **SuSE:** ftp://ftp.suse.com/pub/suse/ **Debian:** http://security.debian.org/pool/updates/main/b/bind/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **EnGarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **ISC:** http://www.isc.org/products/BIND/patches/bind826.diff **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/	BIND Multiple Vulnerabilities CVE Names: CAN-2002-1219, CAN-2002-1220, CAN-2002-1221	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Jacques Gelinas[41]	Unix	Linuxconf 1.2.4 r2, 1.2.5 r3	A vulnerability exists in the configuration file that is created by the mailconf module , which could let a remote malicious user use the system's Sendmail server as a mail relay.	**Conectiva**: ftp://atualizacoes.conectiva.com.br/	Linuxconf mailconf Module Mail Relay	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Jason Orcutt[42]	Windows, Unix	Prometheus 3.0 –beta, 4.0 –beta, 6.0	A vulnerability exists in the prometheus-library/all.lib code due to improper path validation, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Prometheus Framework Code Injection CVE Name: CAN-2002-1211	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Julian Field[43]	Unix	Mail Scanner 3.2 5-1, 3.2 4-1, 3.2 3-1 -3.2.3-5, 4.0 4-1, 4.0 3-1, 4.0 2-3, 4.0 2-2, 4.0 2-1	Two vulnerabilities exist due to the way filenames for attachments are handled, which could let a remote malicious user bypass security checks.	Updates available at: http://www.sng.ecs.soton.ac.uk/mailscanner/downloads.shtml	MailScanner Attachment Filename Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[34] CERT® Advisory CA-2002-31, November 14, 2002.
[35] Conectiva Linux Security Announcement, CLA-2002:546, November 14, 2002.
[36] Debian Security Advisory, DSA 196-1, November 14, 2002.
[37] EnGarde Secure Linux Security Advisory, ESA-20021114-029, November 14, 2002.
[38] FreeBSD Security Advisory, FreeBSD-SA-02:43, November 14, 2002.
[39] Mandrake Linux Security Update Advisory, MDKSA-2002:077, November 14, 2002.
[40] SuSE Security Announcement, SuSE-SA:2002:044, November 14, 2002.
[41] Conectiva Linux Security Announcement, CLA-2002:544, November 6, 2002.
[42] iDEFENSE Security Advisory, 10.31.02b, October 31, 2002.
[43] SecurityTracker Alert ID, 1005572, November 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KDE[44, 45, 46, 47]	Unix	KDE 2.0-2.2, 3.0-3.0.4, klisa 2.2.2; LISa LISa 0.1, 0.1.2	A buffer overflow vulnerability exists in the kdenetwork modules due to insufficient checks on the LOGNAME environment variable, which could let a malicious user obtain root access.	**KDE:** http://download.kde.org/stable/3.0.5/ **Debian:** http://security.debian.org/pool/updates/main/k/kdenetwork/ **LISa:** http://lisa-home.sourceforge.net/src/lisa-0.2.2.tar.bz2 **SuSE:** ftp://ftp.suse.com/pub/suse/	KDE Network Buffer Overflow CVE Name: CAN-2002-1247	High	Bug discussed in newsgroups and websites.
KGPG[48]	Unix	KGPG 0.6-0.8.2	A vulnerability exists because secret keys are generated in an unsafe manner due to the way command line arguments are sent, which could let a malicious user obtain sensitive information.	Upgrades available at: http://devel-home.kde.org/~kgpg/src/kgpg-0.9.tar.gz	KGPG Key Generation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
LBL[49]	Unix	libpcap 0.7.1, tcpdump 3.6.2, 3.7.1	A server hosting tcpdump and libpcap, www.tcpdump.org, was compromised recently and modifications were made to the source code to include Trojan horse code. *Note: Downloads of the source code of tcpdump and libpcap from www.tcpdump.org, and numerous mirrors, likely contain the Trojan code.* The Trojan will run once upon compilation of tcpdump or libpcap. Once the Trojan is executed, it attempts to connect to host 212.146.0.34 on port 1963.	The non-trojaned versions of these tools are available at the following locations: http://www.ibiblio.org/pub/Linux/distributions/gentoo/distfiles/libpcap-0.7.1.tar.gz http://www.ibiblio.org/pub/Linux/distributions/gentoo/distfiles/tcpdump-3.6.2.tar.gz http://www.ibiblio.org/pub/Linux/distributions/gentoo/distfiles/tcpdump-3.7.1.tar.gz	TCPDump / LIBPCap Trojan Horse	Medium	Bug discussed in newsgroups and websites.
LibPNG[50] ***SCO issues patch[51]***	**Unix**	**LibPNG 1.0.12**	**A vulnerability exists due to the way overly wide images are handled, which could let a malicious user execute arbitrary code.**	**Debian:** **http://security.debian.org/pool/updates/main/libp/libpng3** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/**	**LibPNG Wide Image Processing** **CVE Name: CAN-2002-0728**	**High**	**Bug discussed in newsgroups and websites.**

[44] KDE Security Advisory, November 11, 2002.
[45] Gentoo Linux Security Announcement, 200211-004, November 14, 2002.
[46] Debian Security Advisory, DSA 193-1, November 11, 2002.
[47] SuSE Security Announcement, SuSE-SA:2002:042, November 12, 2002.
[48] Gentoo Linux Security Announcement, 200211-002, November 10, 2002.
[49] SecurityFocus, November 13, 2002.
[50] Debian Security Advisory, DSA 140-2, August 5, 2002.
[51] SCO Security Advisory, CSSA-2002-042.0, November 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Light httpd[52]	Windows, Unix	Light HTTPD 0.1	A buffer overflow vulnerability exists when an overly long GET request is submitted, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Light HTTPD Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Linksys Group, Inc.[53]	Multiple	EtherFast BEFSR41 Router 1.40.2, 1.41, 1.42.3, 1.42.7	A Denial of Service vulnerability exists when a malicious user submits a request for the 'Gozila.cgi' script file without any parameters when the default setting is reconfigured to enable "Remote Administration."	Upgrade available at: http://www.linksys.com/download/firmware.asp?fwid=1	Linksys BEFSR41 Denial of Service CVE Name: CAN-2002-1236	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Lotus[54]	Multiple	Lotus Domino 5.0.8, 5.0.9a, 5.0.9	A vulnerability exists when a non-existent NSF database is requested, which could let a remote malicious user obtain sensitive information. *Note: This issue is present on Lotus Domino Server with the 'DominoNoBanner' set to a value of '1'.*	No workaround or patch available at time of publishing.	Lotus Domino NSF Database Banner Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Macro-media, Inc.[55]	Windows NT 4.0/2000, Unix	ColdFusion Server MX Profes-sional, MX Enterprise, MX Developer	A vulnerability exists when the .jsp, .cfm, .cfc, and .cfml extensions mapped to be processed by ColdFusion are not correctly specified during installation, which could let a remote malicious user obtain sensitive information.	**Workaround:** Macromedia suggests when using wsconfig.jar to configure a ColdFusion server, always use the following switch: -map .cfm,.cfc,.cfml,.jsp. For more information, see the Macromedia security bulletin located at: http://www.macromedia.com/v1/Handlers/index.cfm?ID=23499	ColdFusion MX CFML Source Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Macro-media, Inc.[56]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	A buffer overflow vulnerability exists in the IIS ISAPI handler due to insufficient bounds checking on requested filenames, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23500	JRun IIS ISAPI Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[52] INetCop Security Advisory, 2002-0x82-002, November 12, 2002.
[53] iDEFENSE Security Advisory, 10.31.02a, November 6, 2002.
[54] Bugtraq, November 7, 2002.
[55] Macromedia Security Bulletin, MPSB02-13, November 6, 2002.
[56] Macromedia Security Bulletin, MPSB02-12, November 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media, Inc.[57]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	A file disclosure vulnerability exists, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23500	JRun Log File/JRun.INI File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Macro-media, Inc.[58]	Windows 95/98/NT 4.0/2000, Unix	JRun 3.0, 3.1, 4.0	A vulnerability exists due to insufficient validation of Unicode characters in HTTP requests, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.macromedia.com/v1/handlers/index.cfm?ID=23500	JRun Web Server Unicode Source Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
MasqMail [59]	Unix	MasqMail 0.1.16	Two buffer overflow vulnerabilities exist, which could let a malicious user execute arbitrary commands and obtain unauthorized root access.	**Debian:** http://security.debian.org/pool/updates/main/m/masqmail/	MasqMail Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Michael Krax [60]	Unix	log2mail 0.2.5 .0	A buffer overflow vulnerability exists in the 'log2mail' utility, which could let a remote malicious user execute arbitrary code with root privileges.	Update available at: http://security.debian.org/pool/updates/main/l/log2mail/	log2mail Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[57] Macromedia Security Bulletin, MPSB02-12, November 6, 2002.
[58] Macromedia Security Bulletin, MPSB02-12, November 6, 2002.
[59] Debian Security Advisory, DSA 194-1, November 12, 2002.
[60] Debian Security Advisory, DSA 186-1, November 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [61]	Windows 95/98/NT 4.0/2000	JVM 1.1	Multiple vulnerabilities exist: a vulnerability exists in com.ms.security.Standard SecurityManager because the access restriction fields can be altered or emptied, which could let a malicious user bypass security restrictions; a buffer overflow vulnerability exists in class loader when attempting to load a name of excessive length, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; a vulnerability exists because applets are allowed to invoke methods of proprietary Microsoft interfaces, which could let malicious user cause a Denial of Service and possibly execute arbitrary code; a Denial of Service vulnerability exists because the HTML <applet> tag can bypass Java class restrictions; a vulnerability exists in com.ms.vm.loader.Cab Cracker, which could let a malicious user bypass security checks; a vulnerability exists when a Java applet is created with a specially constructed codebase, which could let a remote malicious user obtain sensitive information; a vulnerability exists due to insufficient access validation, which could let a malicious user obtain sensitive information; a vulnerability exists in InativeServices methods, which could let a malicious user cause a Denial of Service and obtain sensitive information; and a vulnerability exists in the parsing of the location URI string, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Microsoft JVM Package Multiple Vulnerabilities	Low/ Medium/ **High** **(Low if a Denial of Service, Medium if sensitive information can be obtained, and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[61] Bugtraq, November 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[62]	Windows NT 4.0/2000	SQL Server 6.0, 6.5, 7.0, 7.0 SP1-SP4, SQL Server 2000, 2000 SP1&2	A vulnerability exists because SQL Server Login passwords are sent across the network using a weak encryption algorithm, which could let a malicious user obtain authentication credentials.	No workaround or patch available at time of publishing.	SQL Server Login Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Mieland, Alexander[63]	Windows, Unix	APBoard 2.0 3, 2.0 2	Two vulnerabilities exist: a vulnerability exists when the 'insertinto' value because messages can be posted to protected forums, which could let a remote malicious user post a thread to a password protected forum; and a vulnerability exists when a user logs in because the plaintext password is included in the forum URL, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	APBoard Protected Forums & Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Monkey[64]	Unix	Monkey HTTP Daemon 0.4-0.4.2, 0.5	A remote Denial of Service vulnerability exists due to inadequate checks when POST requests are decoded.	Upgrade available at: http://monkeyd.sourceforge.net/down.php?vrs=MC41LjE=	Monkey Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[65]	Multiple	D-Link DI-804 4.68, Dl-704 V2.56b6, V2.56b5; Linksys BEFW11S4 1.4.2 .7, EtherFast BEFW11S4 Wireless AP + Cable/DSL Router 1.37.2 b, 1.37.2, 1.37.9 b, 1.40.3, 1.42.7, WAP11 1.3, WAP11 1.4	A Denial of Service vulnerability exists when an overly long HTTP header is sent to the embedded web server.	No workaround or patch available at time of publishing.	Multiple Vendor Embedded HTTP Server Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[62] NTBugtraq, November 2, 2002.
[63] Bugtraq, November 12, 2002.
[64] Securiteam, November 7, 2002.
[65] SecurityFocus, November 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[66]	Unix	Linux kernel 2.4.1-2.4.18	A Denial of Service vulnerability exists when a malicious user triggers a system call with the TF flag enabled.	Upgrade available at: ftp://ftp.kernel.org/pub/linux/kernel/v2.4/linux-2.4.19.tar.bz2	Linux Kernel 2.4 System Call TF Flag Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors [67, 68, 69, 70] ***Conectiva releases patch***[71]	**Unix**	**Debian Linux 2.2, 2.2 sparc, powerpc, IA-32, alpha, arm, 68k, 3.0, 3.0 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, happa, arm, alpha; HP Secure OS software for Linux 1.0; RedHat 6.2, 6.2 sparc, i386, alpha, 7.0, 7.0 i386, alpha, 7.1, 7.1 ia64, i386, 7.2, 7.2 ia64, 7.3, 7.3 i386**	**A vulnerability exists in the 'ypserv' daemon when a malicious Network Information Service (NIS) request is issued, which could let a remote malicious user obtain sensitive information.**	**Debian:** **http://security.debian.org/pool/updates/main/n/nis/** **RedHat:** **ftp://updates.redhat.com/** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/6.0/SRPMS/ypserv-1.3.**	**YPServ Remote Network Information Leakage** **CVE Name: CAN-2002-1232**	**Medium**	**Bug discussed in newsgroups and websites.**

[66] Bugtraq, November 11, 2002.
[67] Debian Security Advisory, DSA 180-1, October 21, 2002.
[68] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:223-07, October 24, 2002.
[69] Hewlett Packard Security Bulletin, HPSBTL0210-074, October 26, 2002.
[70] Gentoo Linux Security Announcement, 200210-010, October 28, 2002.
[71] Conectiva Linux Security Announcement, CLA-2002:539, November 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[72] [73] *More patches released*[74, 75, 76, 77, 78] *Proof of Concept exploit has been published.*[79] *HP releases bulletin*[80] *More patches released*[81, 82, 83, 84, 85]	Windows NT 4.0/2000, Unix	Apache Software Foundation Apache 1.3.20, 1.3.22-1.3.26; Oracle Internet Application Server 1.0.2.1, 1.0.2.0, 8i Enterprise Edition 8.1.7.1.0, 8.1.7.0.0, 9i Application Server, 1.0.2.2, 1.0.2.1s, 1.0.2, 9.0.2, 9.0.2 release 2, 9iAS Reports 9.0.2 .1, Oracle8 8.1.7, 8.1.7.1, 8.1.7, Oracle9i Release 2 9.2 .2, 9.0.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists due to the way the Apache scorecard is handled; a Cross-Site Scripting vulnerability exists due to improper sanitization of SSI error pages, which could let a malicious user execute arbitrary HTML or JavaScript code; and a buffer overflow vulnerability exists in the ab.c web benchmarking support utility, which could let a malicious user execute arbitrary code.	Apache Software Foundation: http://www.apache.org/dist/httpd/apache_1.3.27.tar.gz Oracle Corporation: Oracle has stated that fixes for affected software will be available October 8, 2002 through metalink. *OpenPKG:* ftp://ftp.openpkg.org/release/1.0/UPD/ *Engarde Secure Linux:* ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.32.i386.rpm *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *FreeBSD:* ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/i386/packages-4-stable/All/ *Oracle:* http://metalink.oracle.com *Trustix:* http://www.trustix.net/pub/Trustix/updates/ *Hewlett Packard:* http://www.software.hp.com/ISS_products_list.html *Debian:* http://security.debian.org/pool/updates/main/a/apache/a http://security.debian.org/pool/updates/main/a/apache-ssl *SGI:* ftp://patches.sgi.com/support/free/security/advisories/20021105-01-I	Apache Web Server Multiple Vulnerabilities CVE Names: CAN-2002-0839, CAN-2002-0840, CAN-2002-0843	Low/High (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. *Proof of Concept exploit has been published for the Cross-Site Scripting Vulnerability.*

[72] iDEFENSE Security Advisor, 10.03.2002, October 3, 2002.
[73] OpenPKG Security Advisory, OpenPKG-SA-2002.009, October 4, 2002.
[74] EnGarde Secure Linux Security Advisory, ESA-20021007-024, October 7, 2002.
[75] FreeBSD Security Notice, FreeBSD-SN-02:06, October 10, 2002.
[76] Mandrake Linux Security Update Advisory, MDKSA-2002:068, October 16, 2002.
[77] Oracle Security Alert #45, October 4, 2002.
[78] Trustix Secure Linux Security Advisory, 2002-0069, October 17, 2002.
[79] SecurityFocus, October 30, 2002.
[80] Hewlett-Packard Company Security Bulletin, HPSBUX0210-224, October 30, 2002.
[81] Debian Security Advisory, DSA 187-1, November 4, 2002.
[82] Debian Security Advisory, DSA 188-1, November 5, 2002.
[83] SGI Security Advisory, 20021105-01-I, November 12, 2002.
[84] Debian Security Advisory, DSA 195-1, November 13, 2002.
[85] Gentoo Linux Security Announcement, 200211-003, November 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [86, 87, 88, 89, 90] ***Conectiva releases advisory***[91]	**Unix**	**EnGarde Secure Linux 1.0.1; Mandrake Soft Linux Mandrake 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, 8.2 ppc, 9.0, Single Network Firewall 7.2; mod_ssl mod_ssl 2.4.10, 2.8.9; OpenPKG OpenPKG Current, 1.0, 1.1**	**A Cross-Site Scripting vulnerability exists in mod_ssl where, under certain circumstances, Apache will use the client supplied hostname:port pair, which could let a remote malicious user execute arbitrary HTML and script code.** ***Note: Existence of this vulnerability is limited to configurations with both the 'UseCanonicalName' option turned off and wildcard DNS enabled.***	**EnGarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/i386/apache-1.3.27-1.0.33.i386.rpm** **Mandrake:** **ftp://ftp.planetmirror.com/pub/Mandrake/updates** **OpenPKG:** **ftp://ftp.openpkg.org/** **Debian:** **http://security.debian.org/pool/updates/main/liba/libapache-mod-ssl** ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**	**Mod_SSL Cross-Site Scripting** **CVE Name: CAN-2002-1157**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Multiple Vendors [92, 93, 94, 95, 96, 97] ***RedHat releases patch***[98]	**Unix**	**KTH eBones 1.2, Heimdal 0.3 e, 0.4 a-0.4 e, 0.5, 0.21; MIT Kerberos 4 1.0, 1.1, 4.0, Kerberos 5 1.0, 1.0.6, 1.1, 1.1.1, 1.2-1.2.6; NetBSD NetBSD 1.5-1.5.3, 1.6; OpenBSD OpenBSD 3.0, 3.1**	**A buffer overflow vulnerability exists in the 'kadmind' daemon due to insufficient bounds checking, which could let a remote malicious user obtain root privileges and execute arbitrary code.**	**Debian:** **http://security.debian.org/pool/updates/main/h/heimdal/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **MIT Kerberos:** **http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_patch.txt** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patchees/** **NetBSD:** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-026.txt.asc** ***RedHat:*** **ftp://updates.redhat.com/**	**Multiple Vendor kadmind Remote Buffer Overflow** **CVE Name: CAN-2002-1235**	**High**	**Bug discussed in newsgroups and websites. Exploit is circulating in the wild.** **Vulnerability has appeared in the press and other public media.**

[86] EnGarde Secure Linux Security Advisory, ESA-20021029-027, October 29, 2002.
[87] Debian Security Advisory, DSA 181-1, October 22, 2002.
[88] OpenPKG Security Advisory, OpenPKG-SA-2002.010, October 23, 2002.
[89] Mandrake Linux Security Update Advisory, MDKSA-2002:072, October 24, 2002.
[90] Gentoo Linux Security Announcement, 200210-009, October 27, 2002.
[91] Conectiva Linux Security Announcement, CLA-2002:541, November 6, 2002.
[92] NetBSD Security Advisory, 2002-026, October 21, 2002.
[93] Gentoo Linux Security Announcement, 200210-008, October 26, 2002.
[94] Debian Security Advisory, DSA 183-1, October 29, 2002.
[95] Debian Security Advisory ,DSA 184-1, October 30, 2002.
[96] Mandrake Linux Security Update Advisory, MDKSA-2002:073, October 29, 2002.
[97] MIT krb5 Security Advisory, MITKRB5-SA-2002-, October 26, 2002.
[98] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:242-06, November 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[99], [100]	Mac OS X 10.X, Unix	Apple MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2 (Jaguar), 10.2.1, MacOS X Server 10.0, 10.2-10.2.1; GNU glibc 2.0-2.0.6, 2.1, 2.1.1-6, 2.1.1-2.1.3, 2.1.3-10, 2.2-2.2.5, 2.3, 2.3.1; SGI IRIX 6.5-6.5.13, 6.5.14 m-6.5.17 m, 6.5.14 f-6.5.14 m	A remote Denial of Service vulnerability exists in multiple libc implementations that are based on Sun RPC due to a failure to provide a time-out mechanism when reading data from TCP connections.	**SGI:** ftp://patches.sgi.com/support/free/security/patches/	Multiple Vendor Sun RPC LibC Remote Denial of Service CVE Name: CAN-2002-1265	Low	Bug discussed in newsgroups and websites.
Multiple Vendors[101], [102], [103]	Unix	perl-MailTools 1.13, 1.15, 1.40, 1.42, 1.44, 1.47, 1.1401	A vulnerability exists in a module in the in the perl-MailTools package due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary code.	**SuSE:** ftp://ftp.suse.com/pub/suse/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	PERL-MailTools Remote Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[104], [105], [106], [107],	Unix	FreeBSD 4.5, 4.6; GNU glibc 2.0-2.0.6, 2.1-2.1.3, 2.2-2.2.5	A vulnerability exists due to undersized buffers being passed to res_search() and res_quere(), which could let a malicious user obtain sensitive information.	**FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:42/resolv.patch **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **RedHat:** ftp://updates.redhat.com **NetBSD:** ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-015.txt.asc	Multiple Vendor libc DNS Resolver Information Leakage CVE Name: CAN-2002-1146	Medium	Bug discussed in newsgroups and websites.

[99] CERT/CC Vulnerability Note VU#266817, November 4, 2002.
[100] SGI Security Advisory, 20021103-01-P, November 8, 2002.
[101] SuSE Security Announcement, SuSE-SA:2002:041, November 5, 2002.
[102] Gentoo Linux Security Announcement, 200211-001, November 6, 2002.
[103] Mandrake Linux Security Update Advisory, MDKSA-2002:076, November 7, 2002.
[104] NetBSD Security Advisory 2002-015, October 8, 2002.
[105] Conectiva Linux Security Announcement, CLA-2002:535, November 6, 2002.
[106] FreeBSD Security Advisory, FreeBSD-SA-02:42, November 13, 2002.
[107] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:197-09, November 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Northern Solutions[108]	Windows NT	Xeneo Web Server 2.0.759 .6, 2.1 .0.0	A Denial of Service vulnerability exists when a remote malicious user submits a malformed HTTP request to the web server.	Upgrade available at: http://www.northernsolutions.com/downloads/xeneo_php_setup.exe	Xeneo Web Server Remote Denial of Service CVE Name: CAN-2002-1248	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Novell[109]	Multiple	eMFrame 1.2.1	A buffer overflow vulnerability exists in the user-supplied DN value due to insufficient bounds checking during authentication, which could let a malicious user cause a Denial of Service.	Upgrade available at: http://support.novell.com/servlet/filedownload/ftf/emfrm122.exe/	eMFrame Buffer Overflow	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Novell[110, 111]	Multiple	eDirectory 8.6.2, eDirectory Database 85.20, 85.24, 85.30	A vulnerability exists in Remote Manager when a user's password has expired, which could let a remote malicious user obtain inappropriate privileges.	Upgrade available at: http://support.novell.com/servlet/tidfinder/2963767	eDirectory Expired Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenBSD[112]	Unix	OpenBSD 3.0, 3.1	A Denial of Service vulnerability exists in the getrlimit(2) system call when a malicious user passes a negative value.	Patches available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.0/common/035_kernresource.patch ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/018_kernresource.patch	OpenBSD getrlimit(2) Denial of Service	Low	Bug discussed in newsgroups and websites.
OpenSSH[113]	Unix	OpenSSH	A vulnerability exists because terminal echoing is not disabled when an expired password is required to be renewed, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	OpenSSH Visible Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Pablo Software Solutions[114]	Windows 98/NT 4.0/2000, XP	FTP Server 1.0, 1.2, 1.3, 1.5	A format string vulnerability exists due to inadequate checking of user-supplied login credential input, which could let a remote malicious cause a Denial of Service and possibly execute arbitrary code.	Upgrade to 1.51 available at: http://www.pablovandermeer.nl/ftpserver.zip	FTP Server Format String CVE Name: CAN-2002-1244	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[108] iDEFENSE Security Advisory, 11.04.02b, November 4, 2002.
[109] Novell Security Alert,NOVL-2002-2963651, November 11, 2002.
[110] Novell Security Alert, NOVL-2002-2963767, November 12, 2002.
[111] Novell Security Alert, NOVL-2002-2963827, November 12, 2002.
[112] SecurityTracker Alert ID, 1005553, November 7, 2002.
[113] SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
[114] iDEFENSE Security Advisory, 11.04.02a, November 4, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Padl Software Pty Ltd [115]	Unix	nss_ldap Build 85, 105, 107, 113, 121, 172, 173, 180, 181, 183-192, 194,	Two vulnerabilities exist: a buffer overflow vulnerability exists in the DNS SRV support functions due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and a Denial of Service vulnerability exists due to the way DNS queries are handled.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php	nss_ldap DNS Buffer Overflow & Denial of Service CVE Name: CAN-2002-0825	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Perception [116]	Windows	LiteServe 2.0.1	Several Cross-Site Scripting vulnerabilities exist because the code that produces HTTP directory indices does not properly filter user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	Upgrade available at: www.liteserve.net	LiteServe Input Validation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Perception [117]	Multiple	LiteServe 2.0.1	A Cross-Site Scripting vulnerability exists due to a failure to sanitize query strings from indexed folders, which could let a malicious user execute arbitrary HTML and script code.	Upgrade available at: www.liteserve.net	LiteServe Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Peter Sandvik[118]	Unix	Simple Web Server 0.5.1	A vulnerability exists due to a failure to properly handle malformed URL requests, which could let a malicious user bypass access controls.	No workaround or patch available at time of publishing.	Simple Web Server File Disclosure CVE Name: CAN-2002-1238	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
PHP[119, 120, 121] ***RedHat releases patch***[122]	**MacOS X 10.x, Unix**	**PHP 3.0.14 – 3.0.18, 4.0.3-4.0.7, 4.1.0-4.1.2, 4.2.0-4.2.3**	**A vulnerability exists in the fopen(), file(), and other functions in PHP due to inadequate user input filtering, which could let a remote malicious user create fake HTTP headers by injecting CRLF combinations into HTTP headers using a specially-crafted URL request.**	**Update available at:** **http://cvs.php.net/diff.php/php4/ext/standard/url.c?r1=1.51&r2=1.52&ty=u&Horde=0** **Debian:** **http://security.debian.org/pool/updates/main/p/php3/** **SuSE:** ftp://ftp.suse.com/pub/suse/ ***RedHat:*** **ftp://updates.redhat.com/**	**PHP Function fopen() CRLF Injection** **CVE Name: CAN-2002-0985**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[115] Mandrake Linux Security Update Advisory, MDKSA-2002:075, November 7, 2002.
[116] Bugtraq, November 8, 2002.
[117] Bugtraq, November 8, 2002.
[118] iDEFENSE Security Advisory, 11.08.02a, November 8, 2002.
[119] Securiteam, September 11, 2002.
[120] Debian Security Advisory, DSA 168-1, September 18, 2002.
[121] SuSE Security Announcement, SuSE-SA:2002:036, October 7, 2002.
[122] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:213-06, November 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
QNX Software Systems, Ltd.[123]	Multiple	RTOS 6.1.0	A Denial of Service vulnerability exists when a local malicious user creates multiple timers containing specific characteristics.	No workaround or patch available at time of publishing.	QNX Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
QNX Software Systems, Ltd.[124]	Multiple	RTOS 6.2	A vulnerability exists in a setuid root application packager within QNX because the packaer fails to use absolute paths to execute system commands, which could let a malicious user trick the program into running a trojaned binary and take complete control over a system.	This issue is said to be addressed in the upcoming QNX RTOS 6.2.1 which is expected to be released in January 2003. Concerned customers are advised to contact their QNX representative for information for obtaining a prerelease.	QNX RTOS Application Packager Non-Explicit Path Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Qual-comm, Inc.[125] ***Upgrade released*** *[126]*	**Windows 95/98/NT 4.0/2000**	**Eudora 5.1**	**A vulnerability exists because it is possible to refer to other files or attachments in a message through specially formatted inline text, which could let malicious attachments bypass normal warning dialogs.**	**No workaround or patch available at time of publishing.** ***Upgrade available at:*** **http://www.eudora.com/download/**	**Eudora File Attachment Spoofing**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
RedHat [127] ***SCO releases patch[128]***	**Unix**	**RedHat PXE Server 0.1; HP Secure OS software for Linux 1.0**	**A remote Denial of Service vulnerability exists when a malicious user sends arbitrary Dynamic Host Configuration Protocol (DHCP) packets to the Preboot eXecution Environment (PXE) server from a Voice Over IP (VOIP) phone.**	**RedHat:** **ftp://updates.redhat.com/** **Hewlett Packard:** **The packages listed in RHSA-2002:162 under Red Hat Linux 7.1 i386 are installed to patch HP Secure OS Software for Linux Release 1.0.** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/3.1/**	**Red Hat PXE Server Denial of Service** **CVE Name: CAN-2002-0835**	**Low**	**Bug discussed in newsgroups and websites.**
Research Systems [129]	Windows, Unix	ION Script 1.4	An input validation vulnerability exists in 'ion-p.exe' which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ION Script Remote File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[123] Securiteam, November 7, 2002.
[124] iDEFENSE Security Advisory, 11.08.02b, November 8, 2002.
[125] Bugtraq, August 8, 2002.
[126] Bugtraq, November 13, 2002.
[127] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:162-12, August 30, 2002.
[128] SCO Security Advisory, CSSA-2002-044.0, November 11, 2002.
[129] Bugtraq, November 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RhinoSoft[130]	Multiple	Serv-U 3.0, 3.1, 4.0.0.4	A Denial of Service vulnerability exists when verifying the MKD command.	Upgrade available at: http://www.serv-u.com/download.htm	Serv-U Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Rusty Dragon[131]	Unix	phpBB Advanced Quick Reply Hack 1.0.0, 1.1.0	A vulnerability exists in the 'quick_reply.php' script, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	PHPBB Advanced Quick Reply Hack Remote Code Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Safe.pm[132]	Windows, Unix	Safe.pm 2.0 7, 2.0 6	A vulnerability exists in the Perl 'Safe' module when the Safe module compartment is reused, which could let a local/remote malicious user bypass access restrictions.	Upgrade available at: http://search.cpan.org/author/ABERGMAN/Safe/	Safe.PM Access Bypass	Medium	Bug discussed in newsgroups and websites.
Snort Center[133]	Unix	Snort Center 0.9.5	Two vulnerabilities exist: a vulnerability exists because temporary files are created using predictable file names., which could let a malicious user obtain sensitive information; and a vulnerability exists because temporary sensor configuration files are world readable, which could let a malicious user obtain sensitive information.	Upgrade available at: http://users.pandora.be/larc/download/snortcenter-v0.9.6.tar.gz	SnortCenter Temporary File Access & Insecure Configuration Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Source-craft[134]	Windows, Unix	Networking _Utils 1.0	A vulnerability exists in the ping command due to insufficient sanitization of shell metacharacters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Networking_ Utils Input Validation	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Squirrel Mail[135] ***RedHat issues updated advisory***[136] ***Debian issues advisory***[137]	**Unix**	**Squirrel Mail 1.2.7**	**Multiple Cross-Site scripting vulnerabilities exist in various PHP scripts because user input is not properly sanitized, which could let a malicious user execute arbitrary HTML and script code.**	**Upgrade available at:** **http://prdownloads.sf.net/squirrelmail/squirrelmail-1.2.8.tar.gz** *RedHat:* **ftp://updates.redhat.com/8.0/en/os/noarch/squirrelmail-1.2.8-1.noarch.rpm** ***Debian:*** **http://security.debian.org/pool/updates/main/s/squirrelmail/**	**SquirrelMail Multiple Cross Site Scripting** ***CVE Name: CAN-2002-1131***	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[130] secondmotion-SM-SA-02-03 Security Advisory, November 6, 2002.
[131] Bugtraq, November 13, 2002.
[132] SecurityTracker Alert ID 1005544, November 6, 2002.
[133] Securiteam, November 6, 2002
[134] Bugtraq, November 5, 2002.
[135] Bugtraq, September 19, 2002.
[136] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
[137] Debian Security Advisory, DSA 191-2, November 11, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Squirrel Mail[138] ***Debian issues advisory***[139]	**Unix**	**Squirrel Mail 1.2.7**	**A vulnerability exists in the 'options.php' script when malformed input is provided as arguments, which could let a malicious user obtain sensitive information.**	**Upgrade available at:** **http://prdownloads.sf.net/squirrelmail/squirrelmail-1.2.8.tar.gz** **RedHat:** **ftp://updates.redhat.com/8.0/en/os/noarch/squirrelmail-1.2.8-1.noarch.rpm** ***Debian:*** **http://security.debian.org/pool/updates/main/s/squirrelmail/**	**SquirrelMail Options.PHP** **CVE Name: CAN-2002-1132**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Sun Micro-systems, Inc.[140]	Unix	Solaris 8.0, 8.0_x86, 9.0	A local/remote Denial of Service vulnerability exists which could cause some network interfaces to stop responding to TCP(7P) traffic.	Patches available at: http://sunsolve.sun.com/tpatches	Sun Solaris Local/Remote Denial of Service	**Low**	Bug discussed in newsgroups and websites.
Surecom[141]	Multiple	EP-4501	A vulnerability exists in the default router installation because SNMP (Simple Network Management Protocol) server is enabled with default Community names for read and read/write access, which could let a malicious user cause a Denial of Service or obtain sensitive information.	No workaround or patch available at time of publishing.	EP-4501 Router SNMP Default Community Strings	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites.
SuSE[142] ***Debian issues advisory***[143]	**Unix**	**Linux 7.0-7.3, 8.0, 8.1**	**Two vulnerabilities exist: a vulnerability exists in the 'runlpr' utility when malicious strings are passed via the commandline which could allow a malicious user to execute arbitrary commands; and a vulnerability exists in the html2ps filter that is included in the lprng print system, which could let a remote malicious user execute arbitrary commands.**	**Patches available at:** **ftp://ftp.suse.com/pub/suse/** ***Debian:*** **http://security.debian.org/pool/updates/main/h/html2ps/**	**LPRNG Runlpr & html2ps Command Execution**	**High**	**Bug discussed in newsgroups and websites.**
The Magic Notebook[144]	Unix	The Magic Notebook 1.0 b, 1.1 b	A remote Denial of Service vulnerability exists when a malicious user submits an invalid username.	Upgrade available at: http://jonathanscorner.com/etc/magic_notebook/MagicNotebook1_2.tar.gz	The Magic Notebook Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[138] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:204-10, October 9, 2002.
[139] Debian Security Advisory, DSA 191-2, November 11, 2002.
[140] Sun(sm) Alert Notification, 48601, November 8, 2002.
[141] Arhont Ltd. Information Security Advisory, November 13, 2002.
[142] SuSE Security Announcement, SuSE-SA:2002:040, October 31, 2002.
[143] Debian Security Advisory, DSA 192-1, November 8, 2002.
[144] SecurityTracker Alert ID 1005587, November 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
University of Washington[145]	Unix	Pine 3.98, 4.0.2, 4.0.4, 4.10, 4.20, 4.21, 4.30, 4.33, 4.44	A vulnerability exists when an e-mail message contains a specially crafted FROM: address, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Pine From: Field	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
Windowmaker[146]	Unix	Windowmaker 0.20.1-3, 0.52-2, 0.53, 0.61, 0.61.1, 0.62, 0.62.1, 0.63, 0.63.1, 0.64, 0.65, 0.80	A buffer overflow vulnerability exists in the image handling code, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/w/wmaker/	WindowMaker Image Handling Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Xoops[147]	Unix	WebChat 0.6	A vulnerability exists in the WebChat module due to insufficient sanitization of SQL variables in the 'index.php' script, which could let a remote malicious user execute arbitrary HTML or JavaScript.	No workaround or patch available at time of publishing.	Xoops WebChat Module Remote SQL Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Yahoo![148]	Multiple	Messenger 5.0 .1232, 5.0 .1046	A vulnerability exists in the "Invisible" feature because a remote malicious user can circumvent it.	No workaround or patch available at time of publishing.	Yahoo! Messenger Invisible User Circumvention	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Zeus Technologies[149]	Multiple	Zeus Web Server 4.1r2	A Cross-Site Scripting vulnerability exists due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Zeus Web Server Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

[145] Bugtraq, November 7, 2002.
[146] Debian Security Advisory, DSA-190-1, November 7, 2002.
[147] Securiteam, November 14, 2002.
[148] Bugtraq, November 6, 2002.
[149] Bugtraq, November 8, 2002.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 1 and November 15, 2002, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 18 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 15, 2002	Firewatertoolkit-v97beta.zip	A powerful and comprehensive toolkit for network assessment and defense that scans and maps networks, checks for web vulnerabilities, and includes a powerful, scriptable ISAPI filter (integrates with Snort) for IIS defense.
November 13, 2002	Wds.zip	A DNS ID Spoofer for Windows 9x/2K that lets you use ARP Cache Poisoning tools like winarp_sk or winarp_mim.
November 13, 2002	Wtk.zip	ATCP connection killer for Windows 9x/2K.
November 13, 2002	Wsm.zip	WinSSLMiM implements a HTTPS man-in-the-middle attack from the Windows platform. It includes FakeCert a tool to make fake certificate (like the DCA of sslmim in Phrack 57) and can be used to exploit the Certificate Chain Vulnerability in Internet Explorer.
November 13, 2002	**Libhttpdxpl.c**	**Script which exploits the LibHTTPD POST Buffer Overflow vulnerability.**
November 13, 2002	Lcrzo-4.17.0-src.tgz	A toolbox for network administrators and network malicious users that contains over 200 functionalities using network library lcrzo. For example, one can use it to sniff, spoof, create clients/servers, create decode and display packets, etc.
November 13, 2002	Nmap-3.10ALPHA4.tgz	A utility for port scanning large networks.
November 12, 2002	Dumpwin.zip	A tool that can be used to gather an extensive amount of information about Windows NT/2000 machines, including software, users, ACLs, account lockout policies, running processes, services, etc.
November 12, 2002	Firewar.zip	A tool that can be used to remotely shutdown Windows firewall software such as ZoneAlarm by using ActiveX controls.
November 12, 2002	**Lhttpdxpl.c**	**Light HTTPD Buffer Overflow vulnerability.**
November 7, 2002	**Timer-exploit.c**	**Script which exploits the QNX Denial of Service vulnerability.**
November 3, 2002	**Globalsuntech.c**	**Exploit for the GlobalSunTech Access Point Information Disclosure vulnerability.**
November 3, 2002	**Wcrack2.c**	**Exploit for the GlobalSunTech Access Point Information Disclosure vulnerability.**
November 2, 2002	Xsun-expl.c	Script which exploits the SPARC architecture XSun Heap Overflow vulnerability found in April, 2002.
November 2, 2002	Sneaky-sneaky-1.12.tar.gz	A bi-directional spoofed ICMP tunnel backdoor that has built-in encryption and logging capabilities.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
November 1, 2002	Fdjack.tgz	A multipurpose trace-based file descriptor hijacker for Linux & FreeBSD, with multiple operation modes and "screen -x" style support for TTY hijacking.
November 1, 2002	Forcesql.zip	A SQL server password auditing tool that takes an IP address, user id to check and dictionary file.
November 1, 2002	Ward19.c	A classic war dialer that scans a list of phone numbers, finding the ones where a modem is answering the call. WARD can generate phone numbers lists based on a user-supplied mask, in incremental or random order.

Trends

- **The Internet security community has identified several new vulnerabilities in the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) software, which is used by many ISPs to provide DNS services. The National Infrastructure Protection Center (NIPC) is issuing this advisory to heighten awareness to three newly identified vulnerabilities in BIND versions 4 and 8. For more information see NIPC Advisory 02-009, located at: http://www.nipc.gov/warnings/advisories/2002/02-009.htm and "Bugs, Holes & Patches" table.**
- **The CERT/CC** has received reports that several of the released source code distributions of the libpcap and tcpdump packages were modified by an intruder and contain a Trojan horse. **For more information see CERT® Advisory CA-2002-30, located at: http://www.cert.org/advisories/CA-2002-30.html and "Bugs, Holes & Patches" table.**
- **Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon, which could let a remote malicious user obtain root privileges. The CERT/CC has received reports that indicate that this vulnerability is being exploited. For more information, see "Bugs, Holes & Patches" Table and CERT Advisory, CERT® Advisory CA-2002-29, located at: http://www.cert.org/advisories/CA-2002-29.html.**
- **There have been a significant number of calls from customers concerned about a widespread e-mail that invites users to pick up an "E-Card" from a website called FriendGreetings.com. For more information, see http://www.sophos.com/virusinfo/articles/greetings.html.**
- **Firewalls and other systems that inspect FTP application layer traffic may not adequately maintain the state of FTP commands and responses. As a result, an attacker could establish arbitrary TCP connections to FTP servers or clients located behind a vulnerable firewall. For more information see Vulnerability Note VU#328867, located at: http://www.kb.cert.org/vuls/id/328867.**
- **The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse. For more information, see "Bugs, Holes, & Patches Table" and CERT® Advisory CA-2002-28 located at: http://www.cert.org/advisories/CA-2002-28.html.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of an e-mail-borne worm known as W32.Bugbear or I-Worm.Tanatos. For more information, see NIPC Advisory 02-008, located at: http://www.nipc.gov/warnings/advisories/2002/02-008.htm and Virus Section.**
- **The National Infrastructure Protection Center (NIPC) has been coordinating with the anti-virus and security community on the life cycle of "Slapper," the OpenSSL/Apache worm and all its variants. For more information, see NIPC ASSESSMENT 02-003, located at: http://www.nipc.gov/warnings/assessments/2002/02-003.htm.**
- **The SANS Institute and the National Infrastructure Protection Center (NIPC) have updated the list containing the Twenty Most Critical Internet Security Vulnerabilities. This list is broken into two categories: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. For more detailed information, see: http://www.sans.org/top20.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_JUNBO.A (Batch File Worm): This destructive mass-mailing batch file worm spreads via IRC and the KaZaA peer-to-peer file sharing network. It uses Microsoft Outlook to send e-mail with the following details:

- Subject: Hi!!!
- Message Body: bye!!
- Attachment: casper~1.AVI.bat

This batch file malware overwrites the configuration file, AUTOEXEC.BAT, in the root directory of drive C:\ to display certain text at startup.

I-Worm.Buzill (Internet Worm): This is a worm spreading via the Internet as an attachment to infected e-mails. The worm itself is a Windows PE EXE file about 30KB in length (there is also a known variant that is compressed by UPX, (the compressed size is about 16KB). The Buzill worm is written in Visual Basic. The Subject field is either empty or randomly selected from the various variants. The worm activates from infected e-mails only if a user clicks on the attached file. If this action is taken the worm then installs itself to the system and runs its spreading routine and payload.

I-Worm.Talorm (Internet Worm): This is a worm virus spreading via the Internet as an attachment to infected e-mails and copies itself to IRC channels. The worm itself is a CHM file (compressed HTML file) about 17KB in length. The Subject Line text and body text are randomly selected from the various variants. The worm activates from infected e-mails only when a user clicks on the attached file. If this happens, Talorm then installs itself to the system and runs its spreading routine. he worm then overwrites a registry key with new text:

- HKLM\Software\Microsoft\Windows\CurrentVersion RegisteredOwner = Thalia"

PE_BRID.A (Aliases: Bridex, Braid, W32/Braid@mm, W32/Braid.A-mm, I-Worm.Bridex, W32/Braid-A, Win32.Braid.A, I-Worm.Bridex) (File Infector): This memory-resident program drops the PE infector, PE_FUNLOVE.4099. PE_FUNLOVE.4099 infects Win32 executable files. It also sends copies of itself via Simple Mail Transfer Protocol (SMTP) to all e-mail addresses listed in HTM and DBX files on the infected system. The addresses found are also used to spoof the FROM field of the e-mail message. The details of the e-mail it sends out are as follows:

- From: Registered Owner
- Subject: Registered Organization
- Attachment: README.EXE

This virus does not have a destructive payload.

VBS.Lava (Visual Basic Script Worm): This is a script that is written in Visual Basic. It attempts to delete antiviral program files. VBS.Lava must be downloaded and run to perform its actions. It has no wormlike attributes. When it runs, it first copies itself to C:\Windows\Sooolazo.vbs and C:\WinNT\Sooolazo.vbs. These paths are hard-coded and are not determined by system configuration. If any of the following folders is present on the system, the script attempts to delete all files in the folder:

- C:\AntiViral Toolkit Pro
- C:\Program Files\Command Software\F-PROT95
- C:\Program Files\McAfee\VirusScan
- C:\Program Files\Norton AntiVirus
- C:\Toolkit\FindVirus
- C:\Program Files\Panda Software\Panda Antivirus Titanium

Finally, it adds the values:

- LARVA C:\Windows\sooolazo.vbs
- C:\WinNT\sooolazo.vbs

to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the script runs when you start Windows. The script adds the following lines to Autoexec.bat:

- @Start C:\windows\sooolazo.vbs>nul
- @Start C:\winnt\sooolazo.vbs>nul
- cls

After the script runs, it displays a message box with the title "LVG" and the text, “Error 421 Kernel32.dll.”

VBS/Likun-A (Alias: VBS/Gichty.gen virus) (Visual Basic Script Worm): VBS/Likun-A copies itself to the Windows folder as win32dll.vbs and sets the following registry entry to run itself when Windows starts:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WinLoader32

It then sets the following registry entry to cause Windows to shut down when it starts:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Kernel32 = C:\Windows\rundll32.exe user,exitwindows

It attempts to send itself to all entries in the Windows address book but contains a bug and so does not work successfully. Finally VBS/Likun-A deletes all files with extension MP3 on all drives.

VBS.Melhack.C@mm (Alias: VBS/VBSWG.aw@MM) (Visual Basic Script Worm): This is a Visual Basic Script (VBS) mass mailer. It sends itself to e-mail address that it finds in the Microsoft Outlook Inbox and Sent Mail folders and then deletes e-mail from those folders. The worm also attempts to overwrite some files that have specific extensions. The e-mail will have the following characteristics:

- Subject: XXX Picture For You!
- Attachment: XXX-GIRLS-FOR-YOU.jpg.vbs

VBS_VBSWG.AT (Aliases: VBSWG.AV;VBS/VBSWG@MM, I-Worm.Sdan.b) (Visual Basic Script Worm): This Visual Basic Script (VBS) malware drops a copy of itself in the Windows system directory as WINDOW.JPG.VBS upon execution. It propagates by sending itself as an e-mail attachment using Microsoft Outlook to all recipients found on the infected machine's MS Outlook address book. The details of the e-mail that it sends out are as follows:

- Subject: "º¸°í½Í´Ù Ä£±¸¾ß"
- Message Body: "¹ÙÀÌ·¯½º³¾ß ¿À·£¸¸ÀÌÁö.....È÷È÷"
- Attachment: Window.jpg.vbs

W32.Acint (Alias: W32/Acinti.worm) (Win32 Virus): This is a virus that copies itself to the hard drive and to the floppy disk drive. The existence of the file Cintia.bmp is an indicator of a possible infection. It is written in the Microsoft Visual Basic programming language. When W32.Acint runs, it creates a bitmap file named C:\Cintia.bmp and opens it. It creates the file C:\q, which is only four bytes in length. It may copy itself as the following files:

- C:\%system%\Kernell32.dll.exe
- C:\Archivos de programa\LANSchool\Student.exe
- A:\Cintia.bmp.exe

It adds the value, “Kernell32 C:\%system%\Kernell32.dll.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the virus runs when you start Windows.

W32.Antiqfx.F.Worm (Win32 Worm): This is a minor variant of the W32.Antiqfx.Worm. The two differ only in the size of the worm. The behaviors of both variants are identical. W32.Antiqfx.F.Worm also propagates over the network. The payload deletes files of a specific type and file name. This worm is written in Microsoft C++ and is protected by a HASP layer.

W32.Chili (Win32 Virus): This is a virus that copies itself to the hard drive and to the floppy disk drive. The virus has a standard Windows folder icon to fool unsuspecting users into believing it is really a folder. As a result, when you double-click the icon, the virus is executed. This threat is written in Microsoft Visual Basic programming language. When the virus runs, it copies itself as C:\%system%\System.exe and adds the value, “System C:\%system%\System.exe,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the virus runs when you restart Windows. After the virus runs, it remains in memory, and it examines the floppy disk drive periodically. If it finds a floppy disk in the drive, it copies itself as A:\System.exe.

W32.HLLW.Amazex (Aliases: Worm.P2P.Amazex, TROJ_ANALA.A) (Win32 Worm): This is a worm that attempts to spread across the KaZaA file-sharing network. It disguises itself as a pornographic-related program to trick users into downloading and opening it.

W32.HLLO.Homer.C (Win32 Virus): This is a virus that overwrites files in the Windows folder. The overwritten files become corrupted and are not repairable.

W32.HLLW.Manex (Alias: Win32.Manex) (Win32 Worm): This is a worm that is written in Delphi and C++. When W32.HLLW.Manex runs, it displays a message that begins with the following text: "send 188.1.255.255." It pings random IP addresses of the form 188.1.x.y. If a computer replies to the ping, the worm attempts to infect all disk shares that are on it. When W32.HLLW.Manex infects a share, it looks for .exe files and replaces them with a copy of itself (possibly padded with random data if the original file is larger than the worm executable). If it can not find an .exe file to overwrite, it uses one of the following names when it creates a slightly modified copy of itself on the share:

- <a random number below 999999>.exe
- Animation.exe
- <|ac_f_> - Go Home.exe, where the first few characters in angle brackets may be printed differently on different machines
- Stereo.exe
- DX8Test3D.exe
- Sex&Money.exe

W32.HLLW.Manex listens on port UDP/34251 for a special datagram that triggers the payload if the date is September 1, 2002. When the payload is triggered, the worm performs a Denial of Service attack against IP address 188.1.10.48.

W32.HLLW.Nopadex (Win32 Worm): This is a worm that spreads itself through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic programming language and compressed with tElock. This worm does not have a destructive payload.

W32.Hobble.F@mm (Alias: W32.Alcatap.Worm) (Win32 Worm): This is a variant of the W32.Hobble@mm worm. It attempts to spread across the KaZaA file-sharing network. It also sends itself to e-mail addresses that it retrieves from .htm and .html files that it finds in the Internet Explorer cache, and to all addresses in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: RE:
- Attachment: The e-mail has two attachments. The first one is a copy of the worm, which is 18,432 Bytes in length. The second attachment is a random length text file.

The threat is written in the Microsoft Visual Basic Programming Language and compressed with UPX.

W32/Opaserv-G (Alias: Worm.Win32.Opasoft) (Win32 Worm): This worm has been reported in the wild. It spreads by copying itself to the Windows folder on drive C: and to network shares as INSTIT.BAT. The worm then adds an entry to WIN.INI on the shared drive so that INSTIT.BAT is run when Windows is started. On the infected computer W32/Opaserv-G copies itself to the Windows folder as INSTIT.BAT and adds an entry to the registry at:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm is run when Windows is started. W32/Opaserv-G may also attempt to contact several websites in Brazil.

W32.Poscal.Worm (Aliases: I-Worm.Calposa, WORM_CALPOSA.A, W32/Calposa.worm) (Win32 Worm): This is a worm that attempts to spread itself across KaZaA file-sharing networks. It also attempts to use Microsoft Outlook to send itself to all contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: Anti-Virus Programs are corrupting your Software!
- Attachment:F<??>K_AVs.exe

W32.Stupid.D (Alias: W32.HLLW.Smilex) (Win32 Worm): This is a worm that copies itself to the root folders of all writeable drives. It is written in the Microsoft Visual Basic programming language.

WORM_FREGIT.A (Alias: W32/Fregit@MM) (Internet Worm): This nondestructive worm uses Microsoft Outlook to send itself as attachment to an e-mail it sends to all addresses listed in the Microsoft Outlook address book. This memory-resident worm, written in Visual Basic, arrives in an e-mail as an attachment named "FreeGift.scr." Upon execution, it drops a copy of itself as FreeGift.scr in the Windows system directory. It creates this registry entry so that its dropped copy, FreeGift.scr, automatically executes at Windows startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run FreeGift= %System%\FreeGift.scr

"%System%" is the Windows System directory usually located at C:\Windows\System on Windows 9x/ME systems or at C:\WinNT\System32 on Windows NT/2K/XP systems.

WORM_FRIENDGRT.B (Internet Worm): This variant of WORM_FRIENDGRT.A is a "Friend Greetings" application that sends out an invitation e-mail to the recipients in the infected user's address book, provided that the domain is different from that of the infected user. Once a recipient clicks the URL on this message, he or she is prompted for the installation of this worm program. And as soon as this installation concludes, this worm immediately mass-mails the described message. Other variants of this worm send out the following links instead:

- http://www.<BLOCKED>-greetings.com/pickup/pickup.aspx? code=<sender>&id=<id number>
- http://www.<BLOCKED>-cards.net/pickup/pickup.html? code=<sender>&id=<id number>

WORM_OPASERV.H (Internet Worm): This worm is a variant of WORM_OPASERV.A. It propagates via network shared C:\ drives and attempts to download an executable file from a certain Web site. This file it downloads is usually an update of itself. The download site is currently not accessible and has either been blocked or shut down.

WORM_OROR.C (Aliases: Win32/Roron.C@mm, I-Worm.Roron.31) (Internet Worm): This variant of WORM_OROR.A, propagates by mass-mailing copies of itself to all e-mail addresses it gets from incoming e-mail messages. It also drops copies on shared network drives and terminates certain antiviral, firewall or security applications and deletes files associated with them.

WORM_OROR.D (Aliases: OROR.D, I-Worm.Roron.35) (Internet Worm): This variant of WORM_OROR.A propagates by sending copies of itself via e-mail to all addresses that it gets from incoming e-mail messages of the infected system. It also spreads via shared network drives and Internet Relay Chat. The e-mail that it sends out may contain various subjects. The message body of the e-mail, on the other hand, is randomly selected from an internal list of messages, while the attachment may be any of the various attachments. It also terminates certain antiviral applications and deletes files associated with them. It is written in Visual C++, a high-level programming language.

WORM_OROR.E (Aliases: OROR.E, I-Worm.Roron.37) (Internet Worm): This variant of WORM_OROR.A propagates by sending a copy of itself to all e-mail addresses it gets from the incoming mails of the infected system. It also propagates through MIRC and shared network drives. It terminates certain antiviral, firewall or security applications and deletes files associated with these applications on the infected machine. The e-mail message contains various subjects. The message body of the e-mail that this worm sends out, on the other hand, is randomly selected from an internal list of messages and the attachment contains various names. This variant is also written in Visual C++, a high-level programming language.

WORM_OROR.G (Aliases: IRC_OROR.G, Win32/Roron.G@mm, I-Worm.Roron.gen, OROR.G, W32/Oror.i@MM) (Internet Worm): This variant of WORM_OROR.A, written in Visual C++, uses Simple Mail Transfer Protocol (SMTP) and Mail Application Program Interface (MAPI) to propagate via e-mail. It also propagates via Internet Relay Chat (mIRC) application, local area networks, and through a network shared KaZaA folder. It terminates other antiviral, firewall or security applications and files on its infected machine. The IRC components are detected as IRC_OROR.G.

Worm.P2P.Togod (Internet Worm): This is an Internet worm spreading in the KaZaA peer-to-peer file sharing network. The worm replicates by copying itself into KaZaA shared folder. Togod is a Windows application (PE EXE file) about 100KB in size (compressed by UPX, the decompressed size is about 175KB), written in Delphi. The worm copies itself to the KaZaA directory using the various names. The Togod worm then displays a fake error message:

- Error
- Error loading RCDATA

The worm also creates a randomly named EXE file in the Windows directory where it writes the code for "Backdoor.Lithium" and executes it. Togod also contains the text:

> Hello to all the av's i hope to god norton doesnt detect this first... that would be sad.
> Hell yeah kaspersky!

WORM_PIBI.B (Aliases: PIBI.B, Win32.PiBi.B@mm, W32.Jonbarr.C@mm, W32/Pepex.c@MM**) (Internet Worm):** This worm propagates via e-mail and Internet Relay Chat (IRC). The details of the e-mail that it sends out are as follows:

- From: "Microsoft"
- Subject: WindowsXP Service Release Pack 2.002
- Attachment: install.exe

It also disables antiviral processes and monitoring programs. On the system date, October 18, this worm displays a message box containing various text strings.

Worm/Wlymak (Alias: Worm/Myika.A) (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, the contacts it finds within an ICQ listing. The worm arrives through e-mail in a variety of format disguises itself as coming from an antiviral software vendor. If executed, the worm copies itself in the \windows\ directory under the filename "Setup.exe," as well as, in "C:\Windows\System\Setup32.exe." Additionally, the file "Lymak.exe.bat" gets added in the root directory of C:\. It will then modify lines in the C:\Autoexec .bat file. When the PC is starting up, the worm deletes the following directories with deltree:

- %Windir%\System\*.*
- %Windir%\Start Menu\Programs\Accessories\System Tools*.*
- %Windir%\Cursor\*.*,
- %Windir%\Temp\*.*
- %Windir%\Command\*.*
- %Windir%\System32\*.*

It also deletes the files %Windir%\System.dat and %Windir%\User.dat Finally, if the worm finds one of the following antiviral programs (listed below), it will delete the .dat or .vdf file:

- Kaspersky
- Symantec
- F-Prot
- McAfee
- AntiVir
- Tbav

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Backdoor.AIMVision	N/A	CyberNotes-2002-21
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Antilam.g1	**g1**	**Current Issue**
Backdoor.Armageddon.B	N/A	CyberNotes-2002-20
Backdoor.Asniffer	N/A	CyberNotes-2002-21
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Assasin.B	**B**	**Current Issue**
Backdoor.Baste	**N/A**	**Current Issue**
Backdoor.Bofishy.C	**C**	**Current Issue**
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Cigivip	**N/A**	**Current Issue**
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	N/A	CyberNotes-2002-19
Backdoor.DarkSky.B	B	CyberNotes-2002-20
Backdoor.DarkSky.C	C	CyberNotes-2002-21
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Delf.D	D	CyberNotes-2002-22
Backdoor.Dindang	N/A	CyberNotes-2002-22
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Elitem	N/A	CyberNotes-2002-20
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18

Trojan	Version	CyberNotes Issue #
Backdoor.Feardoor	N/A	CyberNotes-2002-21
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Ana	N/A	CyberNotes-2002-20
Backdoor.FTP_Ana.B	B	CyberNotes-2002-20
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.FunFactory	N/A	CyberNotes-2002-19
Backdoor.GF.13	**N/A**	**Current Issue**
Backdoor.Goster	N/A	CyberNotes-2002-20
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.GWGhost	N/A	CyberNotes-2002-21
Backdoor.Helios	N/A	CyberNotes-2002-19
Backdoor.Hupigeon	N/A	CyberNotes-2002-21
Backdoor.Kaitex.B	B	CyberNotes-2002-20
Backdoor.Kaitex.C	C	CyberNotes-2002-22
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Klb	N/A	CyberNotes-2002-22
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Litmus.203.b	B	CyberNotes-2002-22
Backdoor.Litmus.2a	2a	CyberNotes-2002-20
Backdoor.LittleWitch.B	B	CyberNotes-2002-22
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.Neodurk	**N/A**	**Current Issue**
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Niovadoor	N/A	CyberNotes-2002-22
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	04	CyberNotes-2002-19
Backdoor.Optix.04.b	B	CyberNotes-2002-22
Backdoor.Optix.04.c	C	CyberNotes-2002-22
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.11	11	CyberNotes-2002-20
Backdoor.OptixPro.11.b	B	CyberNotes-2002-22
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Pest.Cli	N/A	CyberNotes-2002-20
Backdoor.Pestdoor	N/A	CyberNotes-2002-20
Backdoor.Phoenix	N/A	CyberNotes-2002-19
Backdoor.Platrash	N/A	CyberNotes-2002-21

Trojan	Version	CyberNotes Issue #
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	N/A	CyberNotes-2002-19
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Revrs	N/A	CyberNotes-2002-22
Backdoor.RMFDoor.Cli	N/A	CyberNotes-2002-20
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Roxrat.10	N/A	CyberNotes-2002-20
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Sdbot.B	B	CyberNotes-2002-22
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Singu	N/A	CyberNotes-2002-22
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	B	CyberNotes-2002-19
Backdoor.Sparta.C	C	CyberNotes-2002-21
Backdoor.Spigot.B	B	CyberNotes-2002-22
Backdoor.Synrg	N/A	CyberNotes-2002-22
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Theef.B	B	CyberNotes-2002-21
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Wiween	N/A	CyberNotes-2002-22
Backdoor.Wold	N/A	CyberNotes-2002-22
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	N/A	CyberNotes-2002-19
Backdoor-AKO	N/A	CyberNotes-2002-20
BackDoor-AKR	N/A	CyberNotes-2002-19
BackDoor-ALT	N/A	CyberNotes-2002-21
BackDoor-AMB	N/A	CyberNotes-2002-22
BackDoor-AMH	**N/A**	**Current Issue**
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	N/A	CyberNotes-2002-19
BDS/Pestdoor.4	N/A	CyberNotes-2002-20
BDS/Sporkbot	N/A	CyberNotes-2002-20
BDS/WinSpyer	N/A	CyberNotes-2002-22
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Cytron	N/A	CyberNotes-2002-20
Diskfill-F	**F**	**Current Issue**
Downloader-BO.b	**b**	**Current Issue**
FakeGina.Trojan	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
Jekord	N/A	CyberNotes-2002-19
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.Antigen	**N/A**	**Current Issue**
PWSteal.BStroj	N/A	CyberNotes-2002-20
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17
PWSteal.SoapSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
QDel297	**N/A**	**Current Issue**
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	N/A	CyberNotes-2002-19
Tr/FakeYahoMe	**N/A**	**Current Issue**
Tr/Mastaz	**N/A**	**Current Issue**
Tr/SCKeyLog.Spy.20	N/A	CyberNotes-2002-22
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/WLoader	N/A	CyberNotes-2002-20
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	N/A	CyberNotes-2002-19
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Bdoor-AML	**N/A**	**Current Issue**
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	N/A	CyberNotes-2002-19
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Netdex-A	N/A	CyberNotes-2002-21
Troj/Nethief-C	N/A	CyberNotes-2002-22
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Unreal-A	N/A	CyberNotes-2002-16
Troj/Zasil-A	**N/A**	**Current Issue**
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_INOR.A	**A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
TROJ_INOR.B	**B**	**Current Issue**
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	N/A	CyberNotes-2002-19
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.AntiUpdater	**N/A**	**Current Issue**
Trojan.Avid	N/A	CyberNotes-2002-19
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	N/A	CyberNotes-2002-19
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.Houpe	**N/A**	**Current Issue**
Trojan.Iblis	N/A	CyberNotes-2002-22
Trojan.IrcBounce	N/A	CyberNotes-2002-19
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	N/A	CyberNotes-2002-19
Trojan.Nullbot	N/A	CyberNotes-2002-19
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	N/A	CyberNotes-2002-19
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.PWS.QQPass.C	N/A	CyberNotes-2002-21
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
Trojan.WinReboot	N/A	CyberNotes-2002-20
UNIX_ALUTAPS.A	N/A	CyberNotes-2002-21
VBS.AVFake	N/A	CyberNotes-2002-22
VBS.Krim.C	N/A	CyberNotes-2002-22
VBS.Lavra.B.Worm	N/A	CyberNotes-2002-19
VBS.Zevach	N/A	CyberNotes-2002-15
VBS/Helvis	N/A	CyberNotes-2002-22
W32.Azak	N/A	CyberNotes-2002-16
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16

Trojan	Version	CyberNotes Issue #
W32.Libi	N/A	CyberNotes-2002-10
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.STD.D	N/A	CyberNotes-2002-22
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15
Worm/Garra	N/A	CyberNotes-2002-20

BackDoor-AMH (Alias: Backdoor.IRC.Mapsy): This remote access server allows an attacker to perform various tasks on the infected system. When the Trojan is run, it copies itself to the WINDOWS SYSTEM (%SysDir%) folder as SysMap.exe and creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "Microsoft® System Mapper"=C:\WINDOWS\SYSTEM\SysMap.exe

It also drops a KeyLogger dll into the system folder, SysMap.dll, and listens on TCP port 6754, for a remote attacker to send various commands. Those commands can perform various tasks on the compromised system.

Backdoor.Antilam.g1 (Aliases: Backdoor.Antilam.g1, BackDoor-AED): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens ports 11831 and 29559 on the infected computer. It is a variant of Backdoor.Antilam. When Backdoor.Antilam.g1 runs, it copies itself as%system%\Foto.exe and creates the value, "foto   C:\WINDOWS\SYSTEM\foto.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. The Trojan attempts to disable some antiviral and firewall programs by terminating their processes. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process, so that it will continue to run after logging off the system. In this case, Backdoor.Antilam.g1 closes only when the system is shut down. In addition, Backdoor.Antilam.g1 attempts to obtain access to the password cache that is stored on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. Once installed, Backdoor.Antilam.g1 waits for commands from the remote client

Backdoor.Assasin.B (Aliases: Backdoor.Assasin.11, Backdoor-AGS, BKDR_SANISI.A): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 6969. The Trojan attempts to disable some antiviral and firewall programs by terminating the active processes.

Backdoor.Baste: This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. Backdoor.Baste is a Delphi application, and is packed with ASPack v2.12. By default it opens port 27374 on the infected computer.

Backdoor.Bofishy.C (Alias: tcpdump Trojan): This is a Trojan that affects the libpcap packet capture library and the tcpdump sniffer. It comes as modified source packages that create a backdoor process during their installation. The backdoor process attempts to contact the attacker's computer and give the attacker access to a shell on the local computer.

Backdoor.Cigivip (Aliases: Backdoor.Cigivip.10, New BackDoor2): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. The Trojan also attempts to send login information for various instant messaging programs to the malicious user. The existence of the file WinSys32.exe is a sign of a possible infection. When Backdoor.Cigivip runs, it copies itself as, ":\Windows\WinSys32.exe," and creates the value, "WinSys32   C:\Windows\Winsys32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan modifies the Win.ini file by adding the line run=C:\Windows\Winsys32.exe so that (on Windows 95/98/Me-based computers) the Trojan starts when you start or restart Windows. The Trojan contains functionality that permits it to retrieve connection information (logon name and password) for these programs:

- MSN Messenger
- Mirabilis ICQ
- AOL Instant Messenger

The retrieved information is then e-mailed to the malicious user.

Backdoor.GF.13 (Alias: Backdoor.GF.13x): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. When Backdoor.GF.13 runs, it may display this message:

- Violation d'acces a l'adresse 00000000. Lecture de l'adresse 00000000.

Then, it copies itself as C:\Windows\Winapp32.exe. Next, it creates the value, " Winapp32.exe C:\WINDOWS\Winapp32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process, so that it continues to run after you log off. In this case, Backdoor.GF.13 will close only when the system is shut down. Once installed, Backdoor.GF.13 waits for commands from the remote client. The commands allow the malicious user to perform any of the following actions:

- Deliver system and network information to the malicious user.
- Open or close the CD-ROM drive and perform other annoying actions.
- Manage the installation of the backdoor Trojan.
- Download and execute files.

Backdoor.Neodurk (Aliases: Backdoor.Neodurk.10, New BackDoor2): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens ports 7673 and 7677. Backdoor.Neodurk is a Delphi application, and it is packed with ASPack v2.001b. When it runs, it copies itself as C:\Windows\Runapp32.exe and creates the value, "Runapp32   C:\Windows\Runapp32.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. If the operating system is Windows 95/98/ME, the Trojan registers itself as a service process to continue to run after you log off. In this case, Backdoor.Neodurk closes only when the system is shut down. In addition, Backdoor.Neodurk attempts to obtain access to the password cache that is stored on the local computer. The cached passwords include modem and dial-up passwords, URL passwords, share passwords, and others. The Trojan installs hook procedures into a hook chain to monitor the system for any keyboard and mouse input. The keyboard and mouse hook procedures process the input and pass the hook information to the next hook procedure in the current hook chain. This permits Backdoor.Neodurk to intercept keystrokes. The Trojan uses e-mail to notify the Trojan client. After Backdoor.Neodurk is installed, it waits for commands from the remote client. The commands allow the malicious user to perform any of the following actions:

- Deliver system and network information to the malicious user.
- Open or close the CD-ROM drive and perform other annoying actions.
- Manage the file system of the infected computer.

Diskfill-F: The Trojan creates multiple large files (containing null data) in order to use up disk space. Subsequently, files (containing only nulls) of size 999,999 bytes are written to the current directory, until the disk is full. The filename used is 'NORTH KOREA DEATH!!.n' (where n = sequential integer).

Downloader-BO.b: This Trojan connects to a prohosting.com user website to download a file named counter. The content of this file is saved locally as OUTPUT.EXE and run. At the time of this writing the downloaded file was a backdoor Trojan, BackDoor-AML. The downloader creates 2 registry keys:

- HKEY_CLASSES_ROOT\.inr\pzeoMm6erZrondFQ "Time"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run ".inr\pzeoMm6erZrondFQ"=%Trojan Path%

A Perl script on the Trojan author's site (on the hypermart.net domain) is accessed, and the country of the infected user is passed to the author.

PWSteal.Antigen (Trojan.PSW.Antigen.c, Antigen.c: This is password-stealing Trojan. It collects user passwords and sends them to the author(s) of the Trojan. Also, the Trojan can be programmed to drop data that has been appended to the Trojan. When PWSteal.Antigen runs, it may create the file, %system%\Gp.dat. This file is not malicious. It contains information that the Trojan collects. The Trojan can also detach any data that has been appended to it, and place it in a temporary folder. This data could take the form of a program, which may or may not be malicious. It can then run the program that it detached. This could be done to appear that a program other than the Trojan is running. If the operating system is Windows 95/98/Me, PWSteal.Antigen attempts to obtain an access to the password cache that is stored on the local computer. The cached passwords include modem and dialup passwords, URL passwords, share passwords, and others. The collected information is then delivered by the Trojan to the author(s) of the Trojan in the form of an e-mail message using its own SMTP client engine. The e-mail message has the following characteristics:

- From: lamer@lamers.org
- To: It sends itself to several addresses that are programmed in the Trojan.
- Attachment: Getpass.txt (Contains the collected cached passwords)

QDel297: This Trojan written in Visual Basic drops an AUTOEXEC.BAT file and forces the victim machine to restart. This runs the dropped AUTOEXEC.BAT file displaying the following string:

- subnix owns you

Subsequently, the deletion of all files from the system drive is attempted using the system tool DELTREE.EXE (with confirmations suppressed).

Tr/FakeYahoMe: This is a keylogger Trojan. It disguises itself as a fake Yahoo! Messenger application. It has the functionality to log keystrokes in gathering users login name and login password. It creates the new file, "C:\Indianhackers.txt." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Yahoo! Pager"="C:\\XXX\\FAKEYAHOOMESSENGER\\YPAGER.exe"

Tr/Mastaz (Aliases: Troj/Maz.A, Maz, Masteraz, Maz.A, Maz.B): This is a Trojan downloader that downloads the file "Msrexe.exe (30.720KB)" from a specified website and installs it in the users \windows\system\ directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "System Service"="C:\\WINDOWS\\SYSTEM\\MSREXE.EXE"

It also adds the key:

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Swartax "ImagePath"="C:\\WINDOWS\\SYSTEM\\MSREXE.EXE"

Troj/Bdoor-AML (Alias: Trojan.PSW.Jeem): This is a backdoor Trojan which allows unauthorized remote access to the computer over a network. The Trojan copies itself to the Windows system folder as MSREXE.EXE and adds an entry to the registry at

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

to run itself on system restart. The Trojan creates the registry entry:

- HKLM\Software\CurrentControlSet\Services\Swartax\ImagePath = "C:\<Windows system>\MSREXE.EXE."

and also creates several registry entries at:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Welcome

Troj/Bdoor-AML attempts to use the affected computer as a proxy SMTP e-mail server. Troj/Bdoor-AML may be dropped by Troj/Dloader-BO.

Troj/Zasil-A (Aliases: Downloader-BN, Trojan.Zasil, TrojanClicker.Win32.Zasil, TROJ/Topmine.A): This Trojan creates and executes the file registry.exe in the Windows folder and then displays a pornographic JPG image. The file registry.exe creates the following registry entry, which starts registry.exe when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Registry Services

Each time registry.exe is executed the Trojan will attempt to download a text file from the internet that contains links to scripts that access pages from lists of website addresses contained in the scripts. The Trojan may also access a spyware script that reports the IP address being used by the active Trojan. Troj/Zasil-A leaves multiple copies of the dropped executable and the JPG file in the Windows Temp folder. The JPG graphic is of a naked middle-aged blonde woman sitting on a table and advertises a pornographic website.

TROJ_INOR.A (Aliases: INOR.A, TrojanDownloader.Win32.Inor, Downloader-BO, TrojanDownloader.Win32.Inor, W32/Maz.A, Tr/Mastaz, Maz, Mastaz, W32/Maz.B): This memory-resident Trojan downloads and executes a backdoor malware from a certain Web site. This backdoor, BKDR_JEEM.A, configures the system to act as an e-mail server that can be used by a remote user to send e-mail. This Trojan spreads as an attached file in forged e-mail messages believed to be sent out intentionally by a malicious sender. Upon execution, this Trojan downloads the file COUNTER.C from the site mas&ltblocked&gtraz.hypermart.net and saves this file as OUTPUT.EXE in the current folder. It then executes this file. If it fails to download the file, it creates the following registry entry:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run .inr\5Nzg1mOWKzFnuvu6 = %Trojan path and filename%

This entry executes this Trojan during Windows startup. This way, it is able to attempt the download every time Windows starts. If the download is successful, it creates the following entry instead:

- HKEY_CLASSES_ROOT\.inr\5Nzg1mOWKzFnuvu6\Done (Default) = “Done”

Regardless of the download results, this Trojan creates the following registry entry:

- HKEY_CLASSES_ROOT\.inr\5Nzg1mOWKzFnuvu6 "Time" = %Hexadecimal equivalent of the time of download%

TROJ_INOR.B (Aliases: TrojanDownloader.Win32.Inor, Troj/Dloader-BO, TrojanDownloader:Win32.Inor): This is a variant of TROJ_INOR.A, a malware that downloads a backdoor, BKDR_JEEM.A, from a certain Web site. The main difference is that this Trojan downloads a malware from a different site and adds a different set of registry keys in the infected system. This malware appears to be spread manually as an attachment to an e-mail message with the following details:

- Subject: Improve your Credit! %Space% %Space%
- Attachment: jimkre.exe

Trojan.AntiUpdater: This Trojan is written as a batch script. When it runs, it attempts to replace the C:\Autoexec.bat file and delete all executable files and some data files in specified folders. The Trojan pretends to be an updater for Symantec virus definitions. When Trojan.AntiUpdater runs, it displays the following message in a DOS window:

> Intelligent Anti-Virus Updater V1.00 -- By Symantec Inc. 28-10-2002.
> Intelligent Anti-Virus Updater is updating your application now, please wait a moment and you must restart the computer may it take effect.
> Updating now, this may take a few minutes ......

After the Trojan displays the message, it sets the system time to 00:00:00 and the system date to January 1, 1980. The Trojan then deletes all executable files and some data files in these folders:

- C:\
- C:\Windows
- C:\Windows\System
- C:\Winnt
- C:\Winnt\System32
- C:\Dos

Finally, the Trojan displays the following message in the same DOS window as the previous message:

> Finished!!! Updater has been updated anti-virus definitions database.

Trojan.Houpe: This is a simple Trojan horse program that is written in Delphi and compressed using a popular program that is used to compress portable executable (PE) files. When Trojan.Houpe runs, it may attempt to steal information from the QQ instant messaging client and send it to the author of the Trojan. When Trojan.Houpe runs, it attempts to copy the following files to the %windir% folder:

- Email.sys
- Info.sys
- Kill.sys
- SMTP.sys
- NotaPad.exe

The Trojan inserts QQ2000B.exe onto the root of the drive from which the Trojan is executed. Next, it modifies the Windows registry so that when you double-click a text file, the Trojan runs. Finally, the Trojan attempts to steal information from the infected computer and send it to the author of the Trojan. The information that it attempts to steal belongs to the QQ instant messaging client.